

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)The Oath accounts walterwallace001@yahoo.com and
chromosome_xv@yahoo.com, more fully described in
Attachment A-1.

Case No. MJ20-662

AMENDED APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A-1, attached hereto and incorporated herein by reference.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B-1, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1343	Wire fraud

The application is based on these facts:

- ☒ See Affidavit of Special Agent Dean Giboney, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

Dean W. Giboney

Applicant's signature

Dean Giboney, Special Agent

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 10/15/2020

Brian A. Tsuchida

Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, Chief United States Magistrate Judge

Printed name and title

STATE OF WASHINGTON)
) SS
COUNTY OF KING)

I. INTRODUCTION AND AGENT BACKGROUND

2. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) for information (including the content of communications) associated with the following accounts (the “Subject Accounts”):

4. The **nwokoro_izundu@hotmail.com** account, the information for which is stored at premises controlled by Microsoft Corporation (“Microsoft”), an email provider located at One Microsoft Way, Redmond, Washington 98052.

1 district court of the United States . . . that – has jurisdiction over the offense being
2 investigated.”

3 III. SUMMARY OF THE AFFIDAVIT

4 10. This investigation arose out of a criminal referral by the Seattle Police
5 Department in April 2019 after one of the victims of a romance scam, Cindy Chen, a Seattle
6 resident, filed a police report. Cindy Chen reported a loss of approximately \$1.5 million to
7 the individual using the alias Henry HASSELHOFF (hereinafter referred to as
8 “HASSELHOFF”). Investigation revealed another victim, Theresa Schwan, a Redmond
9 resident. Theresa Schwan reported a loss of approximately \$285,000 to HASSELHOFF.
10 Both Ms. Chen and Ms. Schwan met HASSELHOFF on the mobile phone dating application
11 Bumble in January 2018. Investigation revealed that an individual going by the name Henry
12 PIERCE (hereinafter referred to as “PIERCE”) used the same phone number to communicate
13 with an additional victim, Kathleen Livesey, who on January 24, 2018, filed a report via
14 telephone with the FBI’s Atlantic City Resident Agency. Livesey reported a loss of
15 approximately \$300,000 to PIERCE. Livesey had met PIERCE on the mobile phone dating
16 application Tinder. Similarities between PIERCE’s and HASSELHOFF’s interactions with
17 these three victims have led investigators to conclude that they are either the same person or
18 co-conspirators.

19 11. HASSELHOFF used one Gmail account to communicate with Ms. Chen and
20 Ms. Schwan. The address for that account is **hasselhoffhenry@gmail.com**. HASSELHOFF
21 used this account to communicate payment directions to the victims as well as to send
22 fraudulent documentation as evidence of the claims he used to obtain financial support from
23 the victims. PIERCE, who is very likely either the same person as HASSELHOFF or
24 HASSELHOFF’s co-conspirator, used a different Gmail account to communicate with Ms.
25 Livesey. The address for that account is **henryderdienstleister@gmail.com**. PIERCE used
26 this account to communicate with Ms. Livesey during and in connection with his romance
27 scam on Ms. Livesey.
28

12. A search warrant executed on Google, Inc. (“Google”) in July 2019 for the **hasselhoffhenry@gmail.com** and **henryderdienstleister@gmail.com** accounts (Case Number MJ19-281) revealed that both accounts used the same secondary or recovery email account of **walterwallace001@yahoo.com**, both accounts were linked to South African telephone numbers, and both accounts showed login activity from the same IP address.

13. A 2703(d) Order compelling production of non-content stored electronic communications for the **walterwallace001@yahoo.com** (Order Number PT20-220) revealed that this account was also being accessed from the same IP address used to login to **hasselhoffhenry@gmail.com** and **henryderdienstleister@gmail.com**, and that email communications were being sent between the **walterwallace001@yahoo.com** account and **hasselhoffhenry@gmail.com** and **henryderdienstleister@gmail.com**.

14. Based on my training and experience, I know that email accounts typically contain evidence of the identity of the person operating the account. Therefore, there is probable cause to believe that the **walterwallace001@yahoo.com** account contains evidence of HASSELHOFF’s and PIERCE’s true identity or identities, as well as evidence of HASSELHOFF/PIERCE’s wire fraud. Moreover, in this case, as described below, there is specific evidence indicating that the **walterwallace001@yahoo.com** account, and its recovery accounts, contain evidence of the identity of the person committing these fraudulent acts.

IV. PROBABLE CAUSE

A. Background on Romance Scams

15. In my training and experience, a romance scam is a form of confidence fraud in which perpetrators often target older women who are divorced or widowed. The Federal Bureau of Investigation’s public website notes that “victims—predominantly older widowed or divorced women targeted by criminal groups usually from Nigeria—are, for the most part, computer literate and educated. But they are also emotionally vulnerable. And con artists know exactly how to exploit that vulnerability because potential victims freely post details about their lives and personalities on dating and social media sites.”

1 16. According to the Federal Trade Commission's Consumer Protection website,
2 warning signs of romance scams include an individual that "professes love quickly; claims to
3 be from the U.S. but is overseas for business or military service; asks for money, and lures
4 you off the dating site; claims to need money for emergencies, hospital bills, or travel; plans
5 to visit but can't because of an emergency." The FTC also notes that reported losses in 2019
6 for romance scams was \$201 million.

7 **B. Cindy Chen**

8 17. In April 2019, the FBI Seattle Division's Complex Financial Crimes squad was
9 contacted by an administrative specialist with the Seattle Police Department regarding a
10 report filed by Cindy Chen in February 2019. The Seattle Police Department General
11 Offense report contained allegations that an individual using the online alias "Henry
12 Hasselhoff" had defrauded Ms. Chen of approximately \$1.5 million from March 2018 to
13 January 2019.

14 18. On April 30, 2019, FBI Special Agents from the Seattle Field Office conducted
15 an interview in person with Cindy Chen. Ms. Chen confirmed the details of the police report
16 she had filed in February and provided additional documentation regarding the fraudulent
17 claims made by HASSELHOFF.

18 19. After meeting Ms. Chen on the dating application Bumble, HASSELHOFF
19 told Ms. Chen he was an engineer currently working on a construction contract for a
20 company called "Hydro-Quebec" in the province of Quebec in Canada. HASSELHOFF
21 additionally claimed that a fire on the construction site at which he worked had caused
22 damage to expensive equipment for which he was responsible, and asked Ms. Chen to help
23 him reimburse his employer. HASSELHOFF provided, via emails sent from the
24 **hasselhoffhenry@gmail.com** account, documents which purported to show his contract
25 with the company as well as the terms of payment for the job. The contract stated that
26 HASSELHOFF would be paid \$800,000.

27 20. HASSELHOFF also represented to Ms. Chen that he had a daughter in
28 Michigan who needed substantial financial support due to a physical disability. At

1 HASSELHOFF's direction, Ms. Chen began sending funds to an individual in Michigan
2 using cashier's checks mailed to a Fed-Ex office store. Ms. Chen used the same method to
3 send funds at HASSELHOFF's direction to an individual in California. On March 24, 2018,
4 Ms. Chen sent the first cashier's check for \$8,000. Ms. Chen sent a total of thirteen cashier's
5 checks between March 24, 2018 and July 18, 2018, totaling \$203,200. HASSELHOFF
6 discussed these payments through communications from the **hasselhoffhenry@gmail.com**
7 account, and sent Ms. Chen the name and address of the individual in California via an April
8 5, 2018 email from the **hasselhoffhenry@gmail.com** account.

9 21. At HASSELHOFF's direction, Ms. Chen then began withdrawing funds from
10 her 401(k) retirement account to send to him. Ms. Chen made a total of six withdrawals from
11 March 8, 2018 to September 6, 2018, for a total of \$925,500, and \$185,100 paid in tax
12 withholdings to the Internal Revenue Service as a result of those withdrawals.

13 22. HASSELHOFF reassured Ms. Chen that he had the funds to repay her "loans"
14 to him. HASSELHOFF directed Ms. Chen to specific websites for multiple banks where
15 HASSELHOFF claimed to have accounts. HASSELHOFF sent this information to Ms.
16 Chen via email from the **hasselhoffhenry@gmail.com** account, and the emails sent to Ms.
17 Chen included login passwords so Ms. Chen could login herself and verify the amount of
18 money he claimed to have. In addition, to gain Ms. Chen's trust and to convince her to
19 continue sending him payments, HASSELHOFF would send Ms. Chen documents that
20 purported to be promissory notes or contracts with terms of repayment for past loans that Ms.
21 Chen had made. HASSELHOFF sent these promissory notes and contracts via emails from
22 the **hasselhoffhenry@gmail.com** account.

23 23. HASSELHOFF also made other false representations regarding his ability to
24 repay Ms. Chen via emails from the **hasselhoffhenry@gmail.com** account. For example, on
25 April 6, 2018, at 6:15 AM, HASSELHOFF emailed Ms. Chen (in relevant part): "Yes I
26 promised 10% interest which will amount to \$1,800 on or before the 16th and I intend to keep
27 my promise. My proposal still stands and that's how it's going to be. I'm sorry for the little
28 mistake. This email is proof I'll be paying back \$19,800 on or before the 16th of April

1 2018.” HASSELHOFF did not pay Ms. Chen \$19,800 (or any amount of money) by April
2 16, 2018. On September 23, 2018, at 9:21 AM, HASSELHOFF emailed Ms. Chen (in
3 relevant part): “As it stands, i owe a total of \$1,633,040 and i promise to payback every
4 single dollar of it. You have my word.” Investigators are not aware of any payments that
5 HASSELHOFF has made to Ms. Chen.

6 24. To further his romance scam, HASSELHOFF also used the
7 **hasselhoffhenry@gmail.com** account to pretend to forward fraudulent emails from various
8 banking institutions. For example, on April 13, 2018, at 6:39 AM, HASSELHOFF emailed
9 Ms. Chen from the **hasselhoffhenry@gmail.com** account, purporting to forward an email
10 from “RBS International Bank” requiring HASSELHOFF to pay an income tax of \$13,405.
11 HASSELHOFF then asked Ms. Chen to send a payment sufficient to cover the purported
12 income tax payment on his behalf. On April 20, 2018, at 6:16 AM, HASSELHOFF sent an
13 email to Ms. Chen from the **hasselhoffhenry@gmail.com** account that stated: “Good
14 morning dear Cindy. I am forwarding you the email I got from the bank manager a few
15 minutes ago.” Below that text is a purported forwarded message from “Jeremy Howard”
16 instructing HASSELHOFF to make two deposits of over \$30,000 into his “premium offshore
17 account” to “successfully complete activation” of that account. Again, HASSELHOFF then
18 asked Chen to send payment sufficient to cover those two deposits over \$30,000.

19 25. Beginning on May 9, 2018, HASSELHOFF also used the
20 **hasselhoffhenry@gmail.com** account to communicate with other email accounts believed to
21 be fraudulent, each time carbon copying Ms. Chen’s email account. Specifically,
22 HASSELHOFF communicated with a “Steve Percy” and “Thomas Cook,” each representing
23 themselves as representatives of Credit Suisse. The email address for “Steve Percy” was
24 **steve.percy@creditsuises.com** and the email address for “Thomas Cook” was
25 **thomas.cook@creditsuises.com**. In my training and experience, scammers typically use fake
26 email addresses with slight misspellings of actual company names—in this case,
27 “creditsuises” rather than “creditsuisse”—when constructing fake online identities with
28 which to further their scam. I believe HASSELHOFF (or his associates or co-conspirators)

1 created these “creditsuises” dummy email accounts for the purpose of furthering the
2 fraudulent scam involving Ms. Chen and, likely, to further other similar scams.

3 26. Ms. Chen never met HASSELHOFF. During most of the period in which they
4 communicated, HASSELHOFF claimed to be either in Canada or in the United Kingdom.
5 He and Ms. Chen would repeatedly plan to meet in person, but HASSELHOFF would
6 repeatedly provide an excuse to avoid a face-to-face meeting. When Ms. Chen, worried
7 about HASSELHOFF’s health given that he had stopped communicating with her, contacted
8 local law enforcement in Liverpool, England in January 2019 to conduct a welfare check on
9 HASSELHOFF, those authorities reported that the address HASSELHOFF had provided to
10 Ms. Chen returned to a construction site, and that HASSELHOFF had never been a patient at
11 the hospital where he told Ms. Chen he had received treatment.

12 27. In my training and experience, the details of Ms. Chen’s experience with
13 HASSELHOFF closely matches a typical romance scam. Ms. Chen is an older, educated
14 woman. HASSELHOFF quickly professed his love for Ms. Chen despite never having met
15 her; quickly moved their communications off of the dating site on which they met; claimed
16 to be overseas during most of their romance; refused to meet Ms. Chen face-to-face, often
17 providing last-minute excuses to cancel plans already made; requested money immediately
18 and in increasing amounts; and claimed to need those funds for emergencies such as tax
19 payments, penalties, and funds for his disabled daughter. In addition, HASSELHOFF’s
20 requests for funds followed a pattern typical, in my training and experience, of online
21 scammers: initial requests for large sums, followed by promises of repayment, followed by
22 additional requests for funds that are supposedly going to enable the victim to be repaid (or
23 even to earn additional money).

24 **C. Theresa Schwan**

25 28. On April 25, 2019, an FBI Special Agent from the Seattle Field Office
26 conducted a telephonic interview with Theresa Schwan. Ms. Schwan provided details of her
27 interactions with the individual using the alias Henry HASSELHOFF.
28

1 29. Ms. Schwan met Henry HASSELHOFF on the dating application Bumble on
2 or about January 23, 2018. They utilized the application's messaging feature for about four
3 days and then moved the majority of their communications to Google Hangouts. Ms. Schwan
4 traveled extensively and used Google Hangouts to keep in touch with HASSELHOFF while
5 she was abroad.

6 30. HASSELHOFF represented to Ms. Schwan that he was an engineer with a
7 contract for a company called "Hydro-Quebec" in Canada. He provided Ms. Schwan
8 documentation of his work contract via the **hasselhoffhenry@gmail.com** account. As with
9 Ms. Chen, HASSELHOFF eventually requested financial assistance from Ms. Schwan,
10 purportedly to deal with a fire at a construction site that resulted in HASSELHOFF's liability
11 for damaged equipment.

12 31. HASSELHOFF additionally told Ms. Schwan that he had a daughter in
13 Cadillac, Michigan, who required financial assistance due to a physical disability.

14 32. At HASSELHOFF's direction and based on the representations noted above,
15 Ms. Schwan sent funds to an individual in California. HASSELHOFF sent an email on April
16 10, 2018, at 6:27 AM, from the **hasselhoffhenry@gmail.com** account, providing Ms.
17 Schwan the address in California to which the funds were to be sent. From the
18 **hasselhoffhenry@gmail.com** account, HASSELHOFF also sent Schwan a promissory note
19 for repayment of \$285,500 on May 15, 2018.

20 33. In my training and experience, the details of Ms. Schwan's experience with
21 HASSELHOFF also closely matches a typical romance scam. Ms. Schwan is an older,
22 educated woman. HASSELHOFF quickly professed his love for Ms. Schwan despite never
23 having met her; quickly moved their communications off of the dating site on which they
24 met; claimed to be overseas during most of their romance; never met Ms. Schwan face-to-
25 face; requested money immediately and in large amounts; and claimed to need those funds
26 for emergencies such as personal liability for an accident or support for his disabled
27 daughter.
28

D. The Flower Shop Payment Records

34. HASSELHOFF sent flower arrangements to both Ms. Chen and Ms. Schwan in February and March 2018, respectively, from Pike Place Flowers, a flower shop located at 1501 1st Avenue, Seattle, Washington. The payment records for both these orders list the **hasselhoffhenry@gmail.com** account as the contact email for the orders.

E. Kathleen Livesey

35. In May 2019, investigative activity revealed a report filed by the FBI's Atlantic City Resident Agency detailing a telephone call received by the duty Agent on January 24, 2018, from Kathleen Livesey of Pleasantville, New Jersey.

36. Ms. Livesey reported that she had sent approximately \$300,000 to an individual using the alias Henry PIERCE, whom she had met on the mobile dating application Tinder in March 2017. Ms. Livesey reported that she and PIERCE had arranged to meet in person numerous times over a 10-month period, but "something came up" each time and they had never met in person. Eventually, PIERCE informed Ms. Livesey that he would send his travel plans to her via text message or email, but Ms. Livesey never received them. PIERCE then cut off all contact with Ms. Livesey. PIERCE used the **henryderdienstleister@gmail.com** account to communicate with Ms. Livesey.

37. PIERCE used the same telephone number to communicate with Ms. Livesey that HASSELHOFF used to communicate with Ms. Chen and Ms. Schwan. In my training and experience, this indicates that the individual or individuals controlling the HASSELHOFF account were the same individual or individuals in contact with Ms. Livesey.

38. Ms. Livesey reported that the individual communicating as PIERCE directed her to send money to "his friend," "Jeremy S. Howard." As recounted earlier, the individual controlling the HASSELHOFF account had also forwarded emails to Ms. Chen from an individual named "Jeremy Howard." In my training and experience, this also indicates that the individual or individuals controlling the HASSELHOFF account were the same individual or individuals in contact with Ms. Livesey.

1 39. On June 17, 2019, an FBI Special Agent from the Seattle Field Office
2 conducted a telephonic interview with Ms. Livesey. Ms. Livesey confirmed the details of
3 the report that she had filed in January 2018 with the Atlantic City Resident Agency. Ms.
4 Livesey recalled that PIERCE told her that he was an engineer, and sent her documentation
5 from his purported employer; he then stated that there was a tragedy on the job site, and that
6 he needed money to help pay for the insurance and the damages. PIERCE claimed that he
7 would pay Ms. Livesey back after he was paid \$800,000 for a contract job. The details of
8 this story—that PIERCE is an engineer, that an accident occurred at the site, requiring
9 immediate funds, and the amount that the employer was purportedly going to pay PIERCE
10 (\$800,000) all closely match the story that HASSELHOFF told Ms. Chen.

11 40. Ms. Livesey recalled that she had sent money to a woman in California and a
12 woman in Michigan at PIERCE's direction. PIERCE told Ms. Livesey that he had a
13 daughter and grandchildren in Michigan that needed financial support. PIERCE's
14 representation that he had a daughter in Michigan who needed financial support, and his
15 instruction to Ms. Livesey that she send money to a woman in California and a woman in
16 Michigan, closely match the representations and instructions made by HASSELHOFF to Ms.
17 Chen and Ms. Schwan. In my training and experience, this also indicates that the individual
18 or individuals controlling the HASSELHOFF account were the same individual or
19 individuals in contact with Ms. Livesey.

20 41. Finally, the FBI's duty Agent reported that PIERCE had provided Ms. Livesey
21 with an eight-digit bank account number with JP Morgan Chase bank, into which Ms.
22 Livesey was to deposit funds. Ms. Chen reported that HASSELHOFF had provided her with
23 a nine-digit bank account number with JP Morgan Chase bank, associated with the individual
24 in California to whom Ms. Chen was instructed to send funds. The eight digits provided by
25 Ms. Livesey are the same as the last eight digits of the nine-digit number provided to Ms.
26 Chen; only the first digit is missing from Ms. Livesey's account number. It is highly likely
27 that the account numbers provided to Ms. Livesey and Ms. Chen were in fact the same, and
28 that the duty Agent simply mistranscribed Ms. Livesey's account number, omitting the first

1 digit. Again, in my training and experience, this also indicates that the individual or
2 individuals controlling the HASSELHOFF account were the same individual or individuals
3 in contact with Ms. Livesey.

4 42. Ms. Livesey declared Chapter 13 Bankruptcy in 2018 after PIERCE failed to
5 repay the approximately \$300,000.

6 43. In my training and experience, the details of Ms. Livesey's experience with
7 PIERCE also closely matches a typical romance scam. Ms. Livesey is an older woman.
8 PIERCE quickly moved their communications off of the dating site on which they met; never
9 met Ms. Livesey face-to-face, despite their making frequent plans to meet; requested money
10 repeatedly and in large amounts; promised to repay those funds; and claimed to need those
11 funds for emergencies such as personal liability for an accident or support for his disabled
12 daughter. Moreover, the fact that PIERCE and HASSELHOFF told Ms. Livesey, Ms. Chen,
13 and Ms. Schwan the same implausible story at different times—that an accident at a job site
14 required huge sums of money to relieve PIERCE or HASSELHOFF of personal liability for
15 the accident—further indicates that that representation was false, as the likelihood of such an
16 accident occurring on multiple occasions is plainly very low.

17 **F. Additional Connections Between E-Mail Accounts**

18 44. A search warrant executed on Google, Inc. ("Google") in July 2019 for the
19 **hasselhoffhenry@gmail.com** and **henryderdienstleister@gmail.com** accounts (Case
20 Number MJ19-281) revealed that both accounts used the same secondary or recovery email
21 account of **walterwallace001@yahoo.com**, both accounts were linked to South African
22 telephone numbers, and both accounts showed login activity from the same Internet Protocol
23 (IP) address (102.182.234.201), which is (according to an open records internet search) also
24 located in South Africa. The **hasselhoffhenry@gmail.com** account had 39 logins or logouts
25 (out of 48 total listed by Google) originating from that IP address. Five other logins or
26 logouts were associate with two other South African IP addresses.

45. The 102.182.234.201 IP address was used regularly to login to the **hasselhoffhenry@gmail.com** account between November 2018 and July 2019 including multiple logins on June 3, 2019, as noted in the following table:

Time	IP Address	Type
2019/06/03-15:27:02-UTC	102.182.234.201	Logout
2019/06/03-15:26:38-UTC	102.182.234.201	Login
2019/06/03-03:55:21-UTC	102.182.234.201	Logout
2019/06/03-03:54:48 -UTC	102.182.234.201	Login

46. The IP log activity provided by Google for the **henryderdienstleister@gmail.com** account was much more limited revealing only one login and one logout for the account. However, these login data points were notable in that they came from the same IP address (102.182.234.201), and were made on June 3, 2019, which is the same date that **hasselhoffhenry@gmail.com** account was accessed from this IP address. The table below shows that IP log data provided by Google for the **henryderdienstleister@gmail.com** account:

Time	IP Address	Type
2019/06/03-15:26:25-UTC	102.182.234.201	Logout
2019/06/03-04:05:11-UTC	102.182.234.201	Login

47. As this example illustrates, these accounts were at times logged into on the same day, and at times one account would be logged off within minutes or seconds of the second account being logged in. Based on that pattern, it is reasonable to believe that the same individual is responsible for this activity, as this pattern is consistent with a single user who can only log into one email account on his internet browser at a time.

48. Google records also revealed that **walterwallace001@yahoo.com** was the secondary or recovery account for 43 additional Google email accounts. Of these accounts, 22 are associated with Nigerian Short Message Service ("SMS") phone numbers and 8 are associated with South African telephone numbers. Many of these accounts such as **heislerhenri@gmail.com**, **mr.henrypierce@gmail.com**, **mr.walterwallace1@gmail.com**,

walterpierce0092@gmail.com, walterwallace149@gmail.com, walterpierce512@gmail.com, walwalll0019@gmail.com, and wwalter746@gmail.com are similar to, or are a combination of, other names used to defraud the victims in this case. Several other accounts, such as brig.markcampbell.usarmy@gmail.com, capt.prinsleypierce.usarmy@gmail.com, kellylinacre.usarmy@gmail.com, and sgt.wvwx11.usarmy@gmail.com give the false impression that they are official U.S. military email accounts, whereas other email accounts such as ahmadsawi.OmanOils@gmail.com, constructionicc9@gmail.com, and walterwallace.austinbank@gmail.com give the appearance that they are related with businesses in the oil, construction or banking industries. In my training and experience, these industries, and spoofed email accounts from these industries, have frequently been used in organized fraud schemes, and more particularly, have been used to target romance scam victims. Additionally, using multiple of these accounts in a coordinated effort can build the trust and confidence of unsuspecting individuals.

49. A 2703(d) Order compelling production of non-content stored electronic communications for the **walterwallace001@yahoo.com** (Order Number PT20-220) revealed that this account was also being accessed from the same IP address used to login to **hasselhoffhenry@gmail.com** and **henryderdienstleister@gmail.com**. Between May 31, 2019 and May 22, 2020, records provided by Oath showed that the same IP address, 102.182.234.201, was used on 34 separate occasions (out of 37 total IP records) to login to the **walterwallace001@yahoo.com** account. In addition, the remaining three IP records were of three other alternative South African IP addresses.

50. A review of email header information provided by Oath showed that there were five outgoing emails from the **walterwallace001@yahoo.com** account to the **hasselhoffhenry@gmail.com** account and one incoming email between May 8, 2018 and February 17, 2020. Similarly, the email header information showed that there were six outgoing emails from the **walterwallace001@yahoo.com** account to the **henryderdienstleister@gmail.com** account between July 29, 2017 and May 27, 2018. Given that the **walterwallace001@yahoo.com** account is the secondary or recovery email

1 for both these accounts, one would not necessarily expect a large volume of email to be sent
2 between the accounts. This low volume of emails between accounts is consistent with the
3 **walterwallace001@yahoo.com** account being utilized by one individual who does not need
4 to often send communications between multiple accounts that he or she controls.

5 51. The search warrant results for the **hasselhoffhenry@gmail.com** and
6 **henryderdienstleister@gmail.com** accounts reveal that the emails sent from the
7 **walterwallace001@yahoo.com** account to those two gmail accounts, though limited in
8 number, include: 1) images of a “Henry Hasselhoff,” 2) forwarded documents associated
9 with “HydroQuebec” that are similar to those used in the scams described in this affidavit,
10 and 3) photos of Amazon gift cards with the PIN numbers scratched off so that they can be
11 redeemed. These communications are thus consistent with the
12 **walterwallace001@yahoo.com** account being used to further the romance scams described
13 above. One particular photograph that was sent from the **walterwallace001@yahoo.com**
14 account to the **hasselhoffhenry@gmail.com** account on June 24, 2018 is the same as a
15 photograph that HASSELHOFF sent to Ms. Chen. This photograph (which depicts an
16 apparently real individual whose identity this target assumed) is depicted below:



26 52. In my training and experience, information, to include stored content, about a
27 secondary, or recovery email account, particularly one that is used as a hub for multiple other
28

accounts involved in fraudulent activity, provides law enforcement officers a better chance of identifying the individual or individuals conducting the fraud as well as other potential victims of the fraud than the account used to contact victims. In my training and experience, perpetrators will attempt to shield their true identity by opening new accounts under fake identities to communicate directly with victims. However, when opening these accounts, perpetrators will often be asked to provide a backup or recovery email. Even if the perpetrators create multiple layers of email accounts under fake identities, at some point within those layers will exist the first email account or set of email accounts the perpetrator opened under a fake identity. That first email account or set of email accounts are more likely to have used the perpetrator's real email account—the email account that the perpetrator holds in their name, or uses to conduct their actual personal business or correspondence—because, at the time the perpetrator opened those first accounts, they had no other fake identity accounts that they could use as a recovery account. Email accounts opened with fake identities can often slowly be unwound to reveal an actual email account with the ultimate user's real identity—if the user has not taken other steps to conceal that identity. Recovery accounts also provide investigators an opportunity to identify other methods being employed to further the fraudulent scheme and determine the extent to which other co-conspirators may be involved in assisting with the scheme.

G. Potential identity of perpetrator

53. Based on the search warrants and 2703(d) Order described above, law enforcement also knows information that may indicate the true identity of the perpetrator of this fraudulent activity. That information is outlined below. However, if indeed this is the true identity of the perpetrator, there is cause to believe the email addresses described below would contain further evidence of that fact, as well as further evidence of the perpetrator's current activities or location.

54. On April 19, 2018, a PDF document was sent from the **hasselhoffhenry@gmail.com** account to the email account **nwokoro_izundu@hotmail.com**. That PDF document is 2 pages long, and displays what

appears to be a Nigerian passport, along with the stamped entry and exit information from that passport. Those two pages are copied below:



55. Several aspects of this passport are notable. First, the passport is a Nigerian passport. As noted above, numerous email accounts associated with the **hasselhoffhenry@gmail.com**, **henryderdienstleister@gmail.com**, and **walterwallace001@yahoo.com** accounts are linked to Nigerian SMS phone numbers. Second, the individual's name (Izundu Victor Arthur Nwokoro) matches the name of the hotmail account to which this was sent, which may indicate that that hotmail account is an account used by this individual to conduct transactions or business using his real identity. Third, the passport includes a departure from Lagos, Nigeria on May 9, 2016, and an entry into South Africa on May 10, 2016. As noted above, one consistent IP address frequently associated with these three accounts (102.182.234.201) is a South African IP address. Moreover, the entry on May 10, 2016 is through the O.R. Tambo International Airport,

1 which is located just outside of Johannesburg, South Africa. The IP address
2 102.182.234.201, according to open-records internet searches, returns to a location also in or
3 just outside of Johannesburg (according to Google Maps, that location is approximately a 20-
4 minute drive from the O.R. Tambo International Airport).

5 56. There are numerous connections between the email accounts used to perpetrate
6 this fraud noted above (the **hasselhoffhenry@gmail.com**,
7 **henryderdienstleister@gmail.com**, and **walterwallace001@yahoo.com** accounts) and
8 email accounts apparently bearing the name Izundu Nwokoro:

9 a. Another email account, **nwokoroizundu@gmail.com**, uses that same
10 individual's name in the account name. Its recovery or secondary account is
11 also **walterwallace001@yahoo.com**.

12 b. From information gleaned from the 2703(d) Order described above, law
13 enforcement knows that emails were sent from the
14 **walterwallace001@yahoo.com** email account to the
15 **nwokoro_izundu@hotmail.com** account (on September 6, 2014) and the
16 **nwokoroizundu@gmail.com** account (on April 13, 2020).

17 c. The **nwokoroizundu@gmail.com** account is also in the contacts list for
18 the **hasselhoffhenry@gmail.com** email account.

19 d. The verified recovery account for **walterwallace001@yahoo.com** is
20 **chromosome_xv@yahoo.com**. The verified alternate or recovery email
21 address for **chromosome_xv@yahoo.com** is **nwokoroizundu@gmail.com**.

22 57. In addition, there are other connections between these accounts and the
23 information shown on the images of the passport detailed above:
24
25
26
27
28

1 a. The subscriber information for **walterwallace001@yahoo.com** lists the
2 user as “Walter Wallace,” with a date of birth listed as May 12, 1970.

3 Nwokoro’s date of birth, as listed on his passport, is May 12, 1992—the same
4 day, but a different year.

5 b. The subscriber information for **chromosome_xv@yahoo.com** lists the
6 user as “Nwokoro Izundu,” with a date of birth of May 12, 1989. Again,
7 Nwokoro’s date of birth from his passport lists the same day (May 12) but a
8 different year (1992). The **chromosome_xv@yahoo.com** account was
9 registered in Nigeria on 02/23/2010, but has recent password changes from
10 05/17/2020 and 06/14/2020 from IP address 102.182.234.201, which is the
11 South African IP address noted above. These dates are consistent with the
12 movement shown on Nwokoro’s passport images from Nigeria to South Africa
13 in 2016. Moreover, of the 380 recent IP addresses associated with activity on
14 the **chromosome_xv@yahoo.com** account, 189 were the 102.182.234.201
15 address noted above.

16 58. Based on the foregoing information, law enforcement believes that “Izundu
17 Nwokoro” may be the real identity of the individual operating these accounts and
18 perpetrating the romance scam frauds described in this affidavit. Law enforcement believes
19 that all of these accounts are likely to contain further information either confirming or
20 refuting that Nwokoro is the real operator of these accounts, and will likely also contain
21 other information that could reveal Nwokoro’s current location, real occupation, and other
22 frauds in which Nwokoro may be engaged.

23 **V. BACKGROUND REGARDING OATH, GOOGLE AND MICROSOFT’S** 24 **SERVICES**

25 **A. Emails**

26 59. In my training and experience, I have learned that Oath, Google, and Microsoft
27 provide a variety of online services, including electronic mail (“email”) access, to the general
28 public. Oath, Google, and Microsoft allow subscribers to obtain email accounts at the

1 domain names “yahoo.com”, “gmail.com”, and “hotmail.com”, respectively, like the email
2 accounts listed in Attachments A-1 through A-3.

3 60. Subscribers obtain an account by registering with Oath, Google, and Microsoft.
4 When doing so, email providers like Oath, Google, and Microsoft ask the subscriber to
5 provide certain personal identifying information. This information can include the
6 subscriber’s full name, physical address, telephone numbers and other identifiers, alternative
7 email addresses, and, for paying subscribers, means and source of payment (including any
8 credit or bank account number). In my training and experience, such information may
9 constitute evidence of the crimes under investigation because the information can be used to
10 identify the account’s user or users, and to help establish who has dominion and control over
11 the account. Indeed, even if the content of emails in an account has been deleted, subscriber
12 information may still be important evidence that would be useful to identify the account’s
13 user or users.

14 61. In my training and experience, email providers typically retain certain
15 transactional information about the creation and use of each account on their systems. This
16 information can include the date on which the account was created, the length of service,
17 records of log-in (i.e., session) times and durations, the types of service utilized, the status of
18 the account (including whether the account is inactive or closed), the methods used to
19 connect to the account (such as logging into the account via the provider’s website), and
20 other log files that reflect usage of the account. In addition, email providers often have
21 records of the Internet Protocol address (“IP address”) used to register the account and the IP
22 addresses associated with particular logins to the account. Because every device that
23 connects to the Internet must use an IP address, IP address information can help identify
24 which computers or other devices were used to access the email account.

25 62. In general, an email that is sent to an Oath, Google, or Microsoft subscriber is
26 stored on the email provider’s servers until the subscriber deletes the email. When the
27 subscriber sends an email, it is initiated at the user’s computer, transferred via the Internet to
28 the email provider’s servers, and then transmitted to its end destination. Email providers

1 often maintain a copy of received and sent emails. Unless the sender specifically deletes an
2 email from the email provider's server, the email can remain on the system indefinitely.
3 Even if the subscriber deletes the email, it may continue to be available on the email
4 provider's servers for some period of time.

5 63. A sent or received email typically includes the content of the message, source
6 and destination addresses, the date and time at which the email was sent, and the size and
7 length of the email. If an email user writes a draft message but does not send it, that message
8 may also be saved by the email provider but may not include all of these categories of data.
9 Users of "yahoo.com" email accounts also have the option to use Yahoo Messenger, a chat
10 function. Based upon my training and experience, all of these types of information may be
11 evidence of crimes under investigation. Stored emails and chats not only may contain
12 communications relating to crimes, but also help identify the participants in those crimes.

13 64. Email providers are also able to provide information that will assist law
14 enforcement in identifying other accounts associated with the Subject Accounts, namely,
15 information identifying and relating to other accounts used by the same subscriber. This
16 information includes any forwarding or fetching accounts¹ relating to the Subject Accounts,
17 all other accounts linked to the Subject Accounts because they were accessed from the same
18 computer (referred to as "cookie overlap"), all other accounts that list the same Short
19 Message Service ("SMS") phone number as the Subject Accounts, all other accounts that list
20 the same recovery email addresses² as do the Subject Accounts, and all other accounts that
21 share the same creation IP address as the Subject Accounts. Information associated with
22 these associated accounts will assist law enforcement in determining who controls the
23

24
25 ¹ A forwarding or fetching account related to the Subject Accounts would be a separate email
26 account that can be set up by the user to receive copies of all of the email sent to the Subject
Accounts.

27 ² The recovery email address is an additional email address supplied by the user that is used by the
28 email provider to confirm your username after you create an email account, help you if you are
having trouble signing into your account or have forgotten your password, or alert you to any
unusual activity involving your email address.

1 Subject Accounts and will also help to identify other email accounts and individuals relevant
2 to the investigation.

3 **B. Customer Service Communications**

4 65. In some cases, email account users will communicate directly with an email
5 service provider about issues relating to the account, such as technical problems, billing
6 inquiries, or complaints from other users. Email providers typically retain records about
7 such communications, including records of contacts between the user and the provider's
8 support services, as well as records of any actions taken by the provider or user as a result of
9 the communications. In my training and experience, such information may constitute
10 evidence of the crimes under investigation because the information can be used to identify
11 the account's user or users.

12 **C. Other Google Services**

13 66. In addition to email and chat, Google offers subscribers numerous other
14 services including: Android, Blogger, Google Alerts, Google Calendar, Google Chrome
15 Sync, Google Cloud Print, Google Developers Console, Google Drive, Google Hangouts,
16 Google Maps, Google Payments, Google Photos, Google Search Console, Google Voice,
17 Google+, Google Profile, Location History, Web & Activity, and YouTube, among others.
18 Thus, a subscriber to a Google account can also store files, including address books, contact
19 lists, calendar data, photographs and other files, on servers maintained and/or owned by
20 Google. For example, Google Calendar is a calendar service that users may utilize to
21 organize their schedule and share events with others. Google Drive may be used to store
22 data and documents, including spreadsheets, written documents (such as Word or Word
23 Perfect) and other documents that could be used to manage a website. Google Photos can be
24 used to create photo albums, store photographs, and share photographs with others and "You
25 Tube," allows users to view, store and share videos. Google Search Console records a
26 Google account user's search queries. And Google Web & Activity records certain browsing
27 history depending on whether the account holder is logged into their account. Like many
28 internet service companies, the services Google offers are constantly changing and evolving.

1 67. Based upon my training and experience, all of these types of information may
2 be evidence of crimes under investigation. Stored emails and chats not only may contain
3 communications relating to crimes, but also help identify the participants in those crimes.
4 Address books and contact lists may help identify co-conspirators. Similarly, photographs
5 and videos of co-conspirators may help identify their true identities, as opposed to supposed
6 identities that they have used in telephone or email communications. Documents may
7 identify the scope of the criminal activity and calendar data may reveal the timing and extent
8 of criminal activity.

9 68. According to Google's website, "Location Reporting" allows Google to
10 periodically store and use a device's most recent location data in connection with the Google
11 Account connected to the device. "Location History" allows Google to store a history of
12 location data from all devices where a user is logged into their Google Account and have
13 enabled Location Reporting. According to Google "[w]hen you turn on Location Reporting
14 for a device like your iPhone or iPad, it lets Google periodically store and use that device's
15 most recent location data in connection with your Google Account." How often Location
16 Reporting updates location data is not fixed. Frequency is determined by factors such as
17 how much battery life the device has, if the device is moving, or how fast the device is
18 moving. Google's location services may use GPS, Wi-Fi hotspots, and cellular network
19 towers to determine an account holder's location.

20 69. Based on the above, I know that if users of the target accounts utilize a mobile
21 device to access the respective Gmail accounts identified in Attachment A-2 and have not
22 disabled location services on their device/s or through the Google account settings, Google
23 may have detailed records of the locations at which the account holders utilized the mobile
24 device(s). This type of evidence may further assist in identifying the account holders, and
25 lead to the discovery of other evidence of the crimes under investigation.

26 **D. Evidentiary Value of Email and Other Content**

27 70. As explained herein, information stored in connection with an email account
28 may provide crucial evidence of the "who, what, why, when, where, and how" of the

1 criminal conduct under investigation, this enabling the United States to establish and prove
2 each element or alternatively, to exclude the innocent from further suspicion. In my training
3 and experience, the information stored in connection with an email account can indicate who
4 has used or controlled the account. This “user attribution” evidence is analogous to the
5 search for “indicia of occupancy” while executing a search warrant at a residence. For
6 example, email communications, contact lists, images sent (and the data associated with the
7 foregoing, such as date and time) may indicate who used or controlled the account at a
8 relevant time. Further, information maintained by the email provider can show how and
9 when the account was accessed or used. For example, as described below, email providers
10 typically log the Internet Protocol (IP) addresses from which users access the email account
11 along with the time and date. By determining the physical location associated with the
12 logged IP addresses, investigators can understand the chronological and geographic context
13 of the email account access and use relating to the crime under investigation. This
14 geographic and timeline information may tend to either inculcate or exculpate the account
15 owner. Additionally, information stored at the user’s account may further indicated the
16 geographic location of the account user at a particular time (e.g., location information
17 integrated into an image or video sent via email). Last, stored electronic data may provide
18 relevant insight into the email account owner’s state of mind as it relates to the offense under
19 investigation. For example, information in the email account may indicate the owner’s
20 motive and intent to commit a crime (e.g., communications relating to the crime), or
21 consciousness of guilt (e.g., deleting communications in an effort to conceal them from law
22 enforcement), and the knowing involvement of other participants in the scheme.

23 71. Pursuant to Title 18, United States Code, Section 2703(g), this application and
24 affidavit for a search warrant seeks authorization to permit Oath, Google, and Microsoft, and
25 its agents and employees, to assist agents in the execution of this warrant. Once issued, the
26 search warrants will be presented to Oath, Google, or Microsoft with direction to identify the
27 accounts described in Attachments A-1 through A-3 to this Affidavit.
28

1 72. The search warrants will direct Oath, Google, or Microsoft to create exact
2 copies of the specified accounts and records. I, and/or other law enforcement personnel will
3 thereafter review the copies of the accounts and records provided by Oath, Google, or
4 Microsoft, and identify from among that content those items that come within the list of
5 items identified on Section II to Attachments B-1 through B-3, for seizure.

6 73. Analyzing the data contained in the accounts may require special technical
7 skills, equipment, and software. It could also be very time-consuming. Searching by
8 keywords, for example, can yield thousands of “hits,” each of which must then be reviewed
9 in context by the examiner to determine whether the data is within the scope of the warrant.
10 Merely finding a relevant “hit” does not end the review process. Keywords used originally
11 need to be modified continuously, based on interim results. Certain file formats, moreover,
12 do not lend themselves to keyword searches, as keywords, search text, and many common
13 email, database and spreadsheet applications do not store data as searchable text. The data
14 may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted
15 by service providers increases, the time it takes to properly analyze recovered data increases,
16 as well. Consistent with the foregoing, searching the recovered data for the information
17 subject to seizure pursuant to this warrant may require a range of data analysis techniques
18 and may take weeks or even months. All forensic analysis of the data will employ only those
19 search protocols and methodologies reasonably designed to identify and seize the items
20 identified in Section II of Attachments B-1 through B-3 to the warrants.

21 74. Based on my experience and training, and the experience and training of other
22 agents with whom I have communicated, it is necessary to review and seize a variety of
23 email communications, chat logs and documents, that identify any users of the Subject
24 Accounts and emails sent or received in temporal proximity to incriminating emails that
25 provide context to the incriminating communications.


26 **VI. REQUEST FOR SEALING**

27 75. I further request that the Court order that all papers in support of this
28 application, including the affidavit and search warrant, be sealed as described in the attached

1 sealing motion. The target of this investigation has used a variety of anonymous web based
2 email accounts, cloud computing services, and other methods to obfuscate his identities
3 while operating an online criminal enterprise. The target of the investigation does not know
4 the full extent of the government's knowledge of their communication channels and email
5 accounts. Much of the evidence in this investigation is electronically stored information. If
6 alerted to the existence of the search warrants, the target under investigation could destroy
7 evidence, including information saved to their personal computers and information stored in
8 other web based email accounts or other online computing accounts. Additionally, if alerted
9 to the existence of the search warrants, the target could change patterns of behavior, notify
10 confederates or take steps to avoid capture and prosecution. Accordingly, there is good
11 cause to seal these documents because their premature disclosure may seriously jeopardize
12 that investigation.

13 VII. CONCLUSION

14 76. Based on the forgoing, I request that the Court issue the proposed search
15 warrant. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not
16 required for the service or execution of this warrant. Accordingly, by this Affidavit and
17 Warrant I seek authority for the government to search all of the items specified in Section I
18 of Attachments B-1 through B-3 (attached hereto and incorporated by reference herein) to
19 the Warrant, and specifically to seize all of the data, documents and records that are
20 identified in Section II to those same Attachments.

21
22 
23 _____
24 Dean W. Giboney, Affiant
25 Special Agent
26 Federal Bureau of Investigation

27 The above-named agent provided a sworn statement attesting to the truth of the
28 contents of the foregoing affidavit over the telephone on the 15th day of October, 2020.



10/15/2020

HONORABLE BRIAN A. TSUCHIDA
Chief United States Magistrate Judge

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A-1

Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the following Oath Holdings, Inc. (“Oath”) accounts (the “Subject Accounts”), that are stored at premises controlled by Oath, a company that accepts service of legal process at 701 First Avenue, Sunnyvale, California:

1. **walterwallace001@yahoo.com**, and any Yahoo Messenger account associated with that email address.

2. **chromosome_xv@yahoo.com**, and any Yahoo Messenger account associated with that email address.

ATTACHMENT B-1

I. Information to be disclosed by Oath, for search:

1. To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Oath, including any emails, records, files, logs, or information that has been deleted but is still available to Oath, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Oath is required to disclose the following information to the government for each of the Subject Accounts listed in Attachment A-1:

a. All electronic mail content and/or preserved data (including email, attachments, and embedded files);

b. All archived Yahoo Messenger content associated with the Subject Account or the user of the Subject Account;

c. All subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Oath in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

d. all contact lists;

e. all account history, including any records of communications between Oath and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified account. This is to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber in connection with the service.

1 2. This Search Warrant also requires Oath to produce the following information
2 (referred to collectively as “Linked Subject Accounts”) for each of the Subject Accounts
3 listed in Attachment A-1:

4 a. a list of all other accounts linked to the Subject Accounts because of
5 cookie overlap with the Subject Accounts;

6 b. a list of all other accounts that list the same SMS phone number as the
7 Subject Accounts;

8 c. a list of all other accounts that list the same recovery email address as
9 the Subject Accounts; and

10 d. a list of all other accounts that shared the same creation IP address as
11 the Subject Accounts within 30 days of creation.

12 3. This Search Warrant also requires Oath to produce the following information
13 for each of the Linked Subject Accounts described in item 2 above of this Attachment B-I:

14 a. Subscriber records for each of the Linked Subject Accounts including 1)
15 names, email addresses, and screen names; 2) physical addresses; 3) records of session times
16 and durations; 4) length of service (including start date) and types of services utilized; 5)
17 telephone or instrument number or other subscriber number or identity, including any
18 temporarily assigned network address such as internet protocol address, media access card
19 addresses, or any other unique device identifiers recorded by Oath in relation to the account;
20 6) account log files (login IP address, account activation IP address, and IP address history);
21 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related
22 accounts.

23 b. All records and other information (not including the contents of
24 communications) relating to the Linked Subject Accounts, including:

25 i. Records of user activity for each connection made to or from the
26 Account(s), including log files; messaging logs; the date time, length, and method of
27 connections, data transfer volume; user names; and source and destination Internet Protocol
28 Addresses; cookie IDs; browser type;

1 ii. Information about each communication sent or received by the
2 Account(s), including the date and time of the communication, the method of
3 communication, and the source and destination of the communication (such as source and
4 destination email addresses, IP addresses, and telephone numbers);

5 iii. All records pertaining to devices associated with the accounts to
6 include serial numbers, model type/number, IMEI, phone numbers, MAC Addresses.

7
8 Oath is hereby ordered to disclose the above information to the government within 14
9 days of service of this warrant.

10
11 **II. Information to be seized by the government:**

12 All information described above in Section I that constitutes evidence and
13 instrumentalities of violations of 18 U.S.C. § 1343 (Wire Fraud), those violations occurring
14 between January 1, 2017 and the present, including, for each account or identifier listed on
15 Attachment A-1, information pertaining to the following matters:

- 16 a. Content that serves to identify any person who uses or accesses the
17 Subject Accounts or who exercises in any way any dominion or control over the accounts;
- 18 b. Content relating to the furtherance of fraudulent requests for funds
19 related to the “romance scam”;
- 20 c. Content that may constitute communications in furtherance of the
21 crimes enumerated above;
- 22 d. Content that may identify assets including bank accounts, commodities
23 accounts, trading accounts, personal property and/or real estate that may
24 represent proceeds of intrusion activity or fraud or are traceable to such
25 proceeds;
- 26 e. Content that may reveal the current or past location of the individual or
27 individuals using the Subject Accounts;
- 28

- 1 f. Content that may reveal the identities of and relationships between co-
2 conspirators;
- 3 g. Content that may identify any alias names, online user names, “handles”
4 and/or “nics” of those who exercise in any way any dominion or control over
5 the specified accounts as well as records or information that may reveal the
6 true identities of these individuals;
- 7 h. Other log records, including IP address captures, associated with the
8 specified account;
- 9 i. Records or information showing the location from which the account
10 user has accessed or utilized the accounts, including GPS, Wi-Fi, or cell tower
11 proximity records related to the accounts;
- 12 j. Address lists or buddy/contact lists associated with the Subject
13 Accounts;
- 14 k. Subscriber records associated with the specified accounts, including 1)
15 names, email addresses, and screen names; 2) physical addresses; 3) records of
16 session times and durations; 4) length of service (including start date) and
17 types of services utilized; 5) telephone or instrument number or other
18 subscriber number or identity, including any temporarily assigned network
19 address such as internet protocol address, media access card addresses, or any
20 other unique device identifiers recorded by Oath in relation to the accounts; 6)
21 account log files (login IP address, account activation IP addresses, and IP
22 address history); 7) detailed billing records/logs; 8) means and source of
23 payment; and 9) lists of all related accounts;
- 24
25
26
27
28

1 l. Records of communications between Oath and any person purporting to
2 be the account holder about issues relating to the accounts, such as technical
3 problems, billing inquiries, or complaints from other users about the specified
4 account. This is to include records of contacts between the subscriber and the
5 provider's support services, as well as records of any actions taken by the
6 provider or subscriber as a result of the communications.

7 m. Information identifying accounts that are linked or associated with the
8 Subject Accounts.

9
10 This warrant authorizes a review of electronically stored information seized, copied, or
11 disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities
12 described in this warrant. The review of this electronic data may be conducted by any
13 government personnel assisting in the investigation, who may include, in addition to law
14 enforcement officers and agents, attorneys for the government, attorney support staff, and
15 technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the
16 seized, copied, or disclosed electronic data to the custody and control of attorneys for the
17 government and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Oath Holdings, Inc. (“Oath”), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Oath. The attached records consist of _____ (pages/CDs/megabytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Oath, and they were made by Oath as a regular practice; and

b. such records were generated by Oath’s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Oath in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Oath, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature